## CLAIMS

What is claimed is:

1. A cryptography engine for performing cryptographic operations on a data block, the cryptography engine comprising:

a key scheduler configured to provide keys for cryptographic operations;

a two-level multiplexer;

expansion logic coupled to the input stage of the multiplexer circuitry, the expansion logic configured to expand a first bit sequence having a first size to an expanded first bit sequence having a second size greater than the first size, the first bit sequence corresponding to a portion of the data block;

permutation logic coupled to the expansion logic, the permutation logic configured to alter a second bit sequence corresponding to the portion of the data block, whereby altering the second bit sequence performs cryptographic operations on the data block.

2. The cryptography engine of claim 1, further comprising an Sbox configured to alter a third bit sequence corresponding to the portion of the data block by compacting the size of the third bit sequence and altering the third bit sequence using Sbox logic.

3. The cryptography engine of claim 1, wherein the cryptography engine is a DES engine.

4. The cryptography engine of claim 1, wherein the multiplexer circuitry comprises two 2-to-1 multiplexers on the first level coupled to two 2-to-1 multiplexers on the second level.

5. The cryptography engine of claim 1, wherein the first bit sequence is less than 32 bits.

6. The cryptography engine of claim 1, wherein the first bit sequence is four bits.

7. The cryptography engine of claim 1, wherein the two-level multiplexer is configured to select either initial data, swapped data, or non-swapped data to provide to the output stage of the multiplexer.

8. The cryptography engine of claim 1, wherein the expansion logic and the permutation logic are associated with DES operations.

9. The cryptography engine of claim 1, wherein the key scheduler performs pipelined key scheduling logic.

10. The cryptography engine of claim 1, wherein the key scheduler comprises a plurality of stages.

11. The cryptography engine of claim 1, wherein the key scheduler comprises a determination stage.

12. The cryptography engine of claim 1, wherein the key scheduler comprises a shift stage.

13. The cryptography engine of claim 1, wherein the key scheduler comprises a propagation stage.

14. The cryptography engine of claim 1, wherein the key scheduler comprises a consumption stage.

15. An integrated circuit layout associated with a cryptography engine for performing cryptographic operations on a data block, the integrated circuit layout providing information for configuring the cryptography engine, the integrated circuit layout comprising:

a key scheduler configured to provide keys for cryptographic operations;

a two-level multiplexer;

expansion logic coupled to the input stage of the multiplexer circuitry, the expansion logic configured to expand a first bit sequence having a first size to an expanded first bit sequence having a second size greater than the first size, the first bit sequence corresponding to a portion of the data block;

permutation logic coupled to the expansion logic, the permutation logic configured to alter a second bit sequence corresponding to the portion of the data block, whereby altering the second bit sequence performs cryptographic operations on the data block.

16. The integrated circuit layout of claim 15, further comprising an Sbox configured to alter a third bit sequence corresponding to the portion of the data block by compacting the size of the third bit sequence and altering the third bit sequence using Sbox logic.

17. The integrated circuit layout of claim 15, wherein the cryptography engine is a DES engine.

18. The integrated circuit layout of claim 1, wherein the multiplexer circuitry comprises two 2-to-1 multiplexers on the first level coupled to two 2-to-1 multiplexers on the second level.

19. The integrated circuit layout of claim 15, wherein the first bit sequence is less than 32 bits.

20. The integrated circuit layout of claim 15, wherein the first bit sequence is four bits.

21. The integrated circuit layout of claim 15, wherein the two-level multiplexer is configured to select either initial data, swapped data, or non-swapped data to provide to the output stage of the multiplexer.

22. The integrated circuit layout of claim 15, wherein the expansion logic and the permutation logic are associated with DES operations.

23. The integrated circuit layout of claim 15, wherein the key scheduler performs pipelined key scheduling logic.

24. The integrated circuit layout of claim 15, wherein the key scheduler comprises a plurality of stages.

25. The integrated circuit layout of claim 15, wherein the key scheduler comprises a determination stage.

26. The integrated circuit layout of claim 15, wherein the key scheduler comprises a shift stage.

27. The integrated circuit layout of claim 15, wherein the key scheduler comprises a propagation stage.

28. The integrated circuit layout of claim 15, wherein the key scheduler comprises a consumption stage.

29. A cryptography engine for performing cryptography operations on a plurality of packets, the packets having payloads and payload gaps, the cryptography engine comprising:

a DES engine;

an asynchronous input buffer coupled to the cryptography engine input;

surrounding logic coupled to the DES engine through the asynchronous input buffer, wherein the DES engine operates at a first clock rate and the surrounding logic operates at a second clock rate different from the first clock rate.

30. The cryptography engine of claim 29, wherein the cryptography engine is coupled to an authentication engine.

31. The cryptography engine of claim 29, wherein the DES engine comprises a two level multiplexer.

32. The cryptography engine of claim 31, further comprising an asynchronous output buffer coupled to the DES engine output.

33. The cryptography engine of claim 31, wherein the asynchronous input buffer is used to convert the data path width from 32-bits to 64-bits.

34. The cryptography engine of claim 31, wherein the asynchronous output buffer is used to convert the data path width from 64-bits to 32-bits.

35. The cryptography engine of claim 31, wherein the input buffer size is determined using the size of the payload gaps and the second clock rate.

36. The cryptography engine of claim 31, wherein the DES engine further comprises a pipelined key scheduler.

37. The cryptography engine of claim 31, wherein the DES engine further comprises inverse permutation logic.

38. The cryptography engine of claim 29, wherein the DES engine is coupled to surrounding logic, wherein the DES engine runs faster than the surrounding logic.

39. The cryptography engine of claim 38, wherein the DES engine and the surrounding logic run at about 500MHz and at about 166MHz, respectively.